Commonwealth of Virginia

Critical Infrastructure Protection and Resiliency Strategic Plan

VIRGINIA LEADING THE WAY

Commonwealth of Virginia
Critical Infrastructure Protection and Resiliency Strategic Plan

VERSION CONTROL LOG

Version	Date of Issue	Authors	Brief Description of Changes
1	December 6, 2007	Secure Commonwealth Panel, Critical Infrastructure Sub-Panel	
2	May 1, 2008	FINAL DRAFT	Formatting—all changes accepted.
	May 2, 2008	Megan Samford—edits after FINAL DRAFT	Final DRAFT—re edit.
	May 3, 2008	Mike McAllister	Final DRAFT-re edit

EXECUTIVE SUMMARY

Central to the mission of the Commonwealth of Virginia is ensuring that communities, businesses, and government are safe, secure, and prepared. Pivotal to the success of this mission is the ability to protect the Critical Infrastructure (CI) and Key Resources (KR) of the Commonwealth. The focus of the *Virginia Critical Infrastructure Protection & Resiliency Strategic Plan* (here fore referred to as the "VA Plan") is the enhancement of CIKR protection and resiliency to ensure that essential governmental missions, state services, and economic functions are maintained in the event of a terrorist attack, natural disaster, or other type of significant incident.

As any significant disaster will entail federal, state, and local involvement, it is critical to establish effective coordination between every level of government. Accordingly, plans and strategies should be synchronized to ensure coordination and cooperation. The Department of Homeland Security (DHS) has provided a coordinated approach through the *National Infrastructure Protection Plan (NIPP)* to "establish national priorities, goals, and requirements for CIKR protection so that federal funding and resources are applied in the most effective manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents." The *Virginia Critical Infrastructure Protection & Resiliency Strategic Plan* has been promulgated to adhere to the tenets of the *National Infrastructure Protection Plan* and to define the Commonwealth's strategy, as well as to direct implementation of supporting plans addressing the specific roles and responsibilities.

The Commonwealth, through the Governor's Office of Commonwealth Preparedness (OCP) will work with federal, state, and local officials, as well as private sector, and Sector Specific Agencies to effect a seamless, coordinated, security and preparedness strategy and supporting implementation plans, as mandated by the General Assembly and the Code of Virginia. In the accomplishment of the same, state agency participation and leadership, coupled with the development and sustainment of strong public-private partnerships, are essential. The primary agencies responsible for coordinating the fulfillment of critical infrastructure program requirements and initiatives, as well as the response to and recovery from events that have impacts upon the Commonwealth's CIKR, are depicted in Figure ES-1. Their subject matter experts will support the Governor's Office of Commonwealth Preparedness Critical Infrastructure Program (CIP) efforts. Their continued involvement in coordination and collaboration regarding CIP, which will be enhanced by efforts from other state agency resources, will be central to future preparedness efforts. By proactively coordinating and collaborating at appropriate levels of government, public sector organizations, private industry, etc., CIP will be enhanced along with a "unity of results" that comes from a "unity of effort."

Commonwealth Coordinating Agencies	
Oversight of implementation of DHS strategies to develop integrated plans to unify and enhance CIKR protection	• Office of Commonwealth Preparedness (OCP)
Primary Agencies	• Department of State Police (VSP) • Virginia Department of Emergency Management (VDEM) • Virginia Department of Transportation (VDOT)

Figure ES-1. Responsible Agencies

The protection of the Commonwealth's CIKR is essential for making Virginia and the Nation safer, more secure, and more resilient in the context of an all-hazards approach including natural and manmade disasters. Protection includes actions to mitigate the overall risk to physical, cyber, and human CIKR assets, systems, networks, functions, or their interconnecting links resulting from: exposure, injury, destruction, incapacitation, or exploitation. This includes actions to deter threats, mitigate vulnerabilities, as well as minimize consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities such as improving business protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, leveraging "self-healing" technologies, promoting workforce surety programs, or implementing cyber security measures, among various others. The *National Infrastructure Protection Plan* and its complementary Sector-Specific Plans provide a consistent, unifying structure for integrating both existing and future CIKR protection efforts. This information will provide the Commonwealth with the core processes and mechanisms that enable all levels of government and private sector security partners to work together to implement CIKR protection in an effective and efficient manner.

The *VA Plan* will address the following: Authorities, Roles, and Responsibilities; CIKR Protection Program Strategy; Organizing and Partnering for CIKR Protection; CIKR Protection; Ensuring an Effective, Efficient Program Over the Long Term; and Providing Resources for the CIKR Protection Program.

Figure ES-2 depicts the relationships and essential tasks that are key to affecting the *VA Plan*. Notwithstanding federal requirements, Executive Order 44, § 44-146.17 mandates the incorporation of emergency planning into the culture of all state agencies. Accordingly, the Governor directs the Secretaries to implement the tenets of the *VA Plan*. In turn, cognizant agencies will implement the *VA Plan* by reviewing the Federal Sector-Specific Plan considerations in the *Summary of the National Infrastructure Protection Plan and Sector Specific Plans* and the State Sector-Specific Plan considerations in Appendix A. The Secretaries will engage their Agencies and Departments to partner with the private sector entities whose involvement is considered key to the protection of the relevant CI. This is done by National, State, Regional and local coordination that is appropriate to the organizations involved taking into consideration practices, nuances, and idiosyncrasies that are unique to the sector. Furthermore, efficient and secure communications must be put in place to ensure the timely receipt of sector critical information, but also the safeguarding of the same. It is the intent of this partnership of public and private entities to explore the most effective methods to employ and to craft a plan that ensures the resiliency of the CIKR. As a

result of meetings, coordination, and planning, a Sector-Specific Plan will be promulgated.

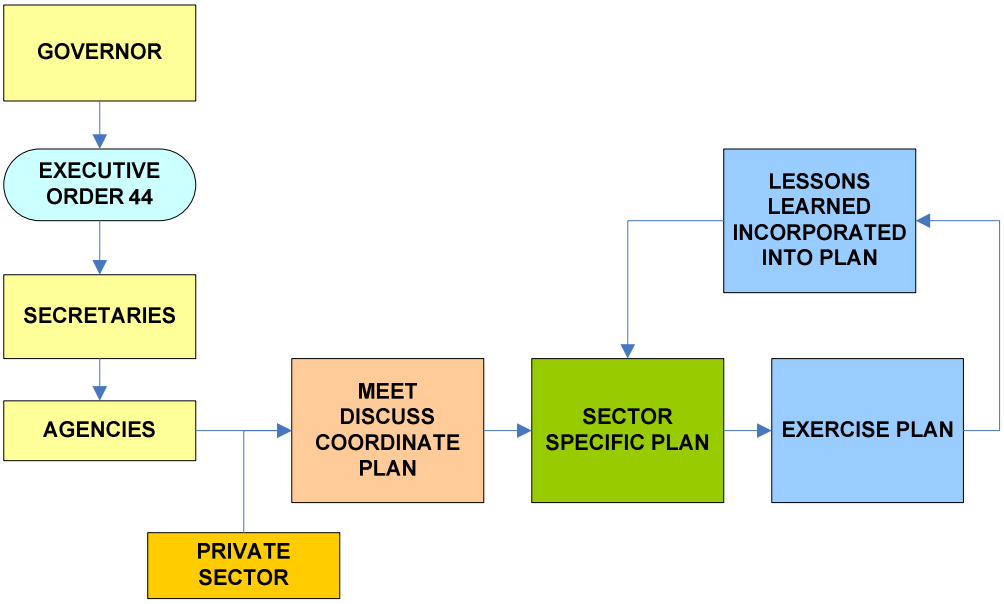

Figure ES-2. VA PLAN Process

Once all plans are in place, OCP will review the plans for completeness and interdependencies. However, a plan must be responsive to changing conditions, and a plan must be exercised to ensure efficacy and relevancy. Lessons learned as a result of a robust exercise schedule are used to change the plan, making it and the CIKR it is meant to protect more resilient. This process is more thoroughly examined and illustrated in Chapter 1.

OCP will maintain and monitor Administrative Goals and Priorities encapsulating the responsibilities of the Sector-Specific Agencies. Sector-Specific Goals and Priorities will be provided by OCP as guidelines to the Sector-Specific Agencies for the development of Sector-Specific Plans. Armed with the information contained in the *VA Plan* and following the basic procedures described above, Commonwealth Agencies and Departments will be able to construct the Sector-Specific Plans that are essential to our security.

Robert P. Crouch, Jr.
Assistant to the Governor
for Commonwealth Preparedness

LETTER OF AGREEMENT

The Commonwealth of *Virginia Critical Infrastructure Protection and Resiliency Strategic Plan (VA Plan)* provides an overarching structure for the integration of Critical Infrastructure and Key Resources (CIKR) protection into a Commonwealth program that reflects the framework defined in the Department of Homeland Security (DHS) National Infrastructure Protection Plan. The *VA Plan* provides a Commonwealth-wide structure for programs and activities that are currently underway in the various sectors, as well as new and developing CIKR protection efforts. This collaborative effort between the private sector, federal and local governments, nongovernmental organizations, and the Commonwealth, will result in the prioritization of protection initiatives and investments across sectors within the Commonwealth of Virginia. It will ensure that resources are applied where they offer the most benefit for protection and resiliency by lowering vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other incidents.

By signing this letter of agreement, Sector-Specific Agencies and other Commonwealth entities and agencies with special functions related to CIKR protection will indicate their understanding of their responsibility to support *VA Plan* concepts, frameworks, and processes, and carry out their assigned functional responsibilities as appropriate and consistent with their own department-specific authorities, resources, and programs regarding the protection of CIKR as described below:

- Appoint a Sector Lead for each assigned sector to work with the Office of Commonwealth Preparedness as part of the VA Plan Coordinating Council;
- Work with the Office of Commonwealth Preparedness to coordinate funding and implementation of programs that enhance CIKR protection;
- Provide annual reports, or more frequently if conditions warrant, to the Office of Commonwealth Preparedness on their efforts to identify, prioritize, and coordinate CIKR protection in their respective sectors;
- Coordinate development of Sector-Specific Plans in collaboration with security partners and submit completed Sector-Specific Plans to the Office of Commonwealth Preparedness within 180 days of final approval of the *VA Plan*. Each Sector-Specific Plan will align with the *VA Plan* risk management framework and include a menu of sector-specific protective activities and a description of the sector's information-sharing mechanisms and protocols;
- Develop or modify existing interagency and agency-specific CIKR plans, as appropriate, to facilitate compliance with the *VA Plan* and Sector-Specific Plans;
- Develop and maintain partnerships for CIKR protection with appropriate federal, Commonwealth, regional, and local entities; the private sector; and nongovernmental organizations (NGO) as described herein; and
- Protect critical infrastructure information according to the Protected Critical Infrastructure Information program and/or other appropriate guidelines, and share information relevant to CIKR protection (e.g., actionable information on threats,

incidents, CIKR status, etc.) as appropriate and consistent with their own agency-specific authorities and the processes described herein.

Critical Infrastructure/Key Resources (CIKR) Sector	Secretariats	Virginia's Sector Specific Agencies (As assigned by OCP)
Agriculture and Food	Agriculture and Forestry	Department of Agriculture and Consumer Services Department of Health
Defense Industrial Base	Public Safety Transportation	National Guard Department of Military Affairs
Energy	Natural Resources	Department of Mines, Minerals and Energy State Corporation Commission
Public Health and Healthcare	Health and Human Resources	Department of Health Department of Environmental Quality
National/State Monuments and Icons	Natural Resources	Department of Conservation and Recreation Virginia Tourism Corporation Department of Historic Resources State Council of Higher Education for Virginia
Banking and Finance	Finance	Department of the Treasury State Corporation Commission
Drinking Water and Water Treatment Systems	Health and Human Resources	Department of Health Department of Environmental Quality
Chemical	Health and Human Resources	Department of Health Department of Environmental Quality Department of Emergency Management Department of State Police Department of Agriculture and Consumer Services
Commercial Facilities	Commerce and Trade	Department of Business Assistance Virginia Tourism Corporation Virginia Economic Development Partnership
Dams	Natural Resources	Department of Conservation and Recreation Department of Game and Inland Fisheries
Emergency Services	Public Safety	Department of Emergency Management Department of State Police
Commercial Nuclear Reactors, Materials, and Water	Natural Resources Public Safety	Department of Conservation and Recreation Department of Game and Inland Fisheries Department of Emergency Management Department of State Police Department of Health
Information Technology	Technology	Information Technologies Agency
Telecommunications	Technology	Information Technologies Agency State Corporation Commission
Postal and Shipping	Transportation	Department of Transportation
Transportation Systems	Transportation	Department of Transportation

Critical Manufacturing	Commerce and Trade	Department of Business Assistance Virginia Economic Development Partnership Department of Transportation
Government Facilities	Administration	Department of General Services Department of State Police Department of Military Affairs

Figure 1. CIKR Sectors, Secretariats, and Corresponding Agencies and Departments

Figure 2. Signatories

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1 INTRODUCTION

The protection of the Commonwealth's critical infrastructure (CI) and key resources (KR) constitutes a multi-faceted endeavor. In order to manage risks, such as deterring threats, mitigating vulnerabilities, and minimizing consequences, myriad activities must take place (Figure 3). Examples of these activities include: developing plans, training, enhancement of resiliency and personnel surety. The *Virginia Critical Infrastructure Protection & Resiliency Strategic Plan (hereafter referred to as the "VA Plan")* contained herein with its complementary Sector-Specific Plans provides the overarching architecture with which to integrate existing and future CIKR protection efforts.

Figure 3. Protection Matrix

1.1 Purpose

The purpose of the *VA Plan* is to set forth the strategy for Commonwealth agencies to follow in the pursuit of greater security and resiliency for the State's CIKR by providing the information required to understand security needs, identify vulnerabilities, and to craft cogent, executable, Sector-Specific Plans.

1.2 Scope

The *VA Plan* is consistent with the policy direction established in the National Infrastructure Protection Plan (NIPP), the Homeland Security Presidential Directive 7 (HSPD-7), the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, the National Strategy to Secure Cyberspace, and Governor Kaine's Executive Order 44. The core focus of the *VA Plan* is the protection of CIKR from the unique and potentially catastrophic impacts of terrorist attacks, which is consistent with the Commonwealth's all-hazards approach to homeland security preparedness and domestic incident management.

1.3 Applicability

The VA Plan embraces the concepts of the National Infrastructure Protection Plan. The National Infrastructure Protection Plan covers the full range of CIKR sectors defined in HSPD-7 and is applicable to the various public and private sector security partners in different ways. The framework is applicable to all security partners with CIKR protection responsibilities and includes explicit roles and responsibilities for the Federal Government, including CIKR under the control of independent regulatory agencies, and the legislative, executive, or judicial branches. Other federal departments and agencies with specific responsibilities for CIKR protection are required by the National Infrastructure Protection Plan to take actions consistent with HSPD-7. The National Infrastructure Protection Plan also provides an organizational structure, protection

guidelines, and recommended activities, for security partners to help ensure consistent implementation of a national framework and the most effective use of resources. The VA Plan satisfies the State, local, and security partners requirements to establish CIKR protection programs that are consistent with the National Preparedness Goal and as a condition of eligibility for certain federal grant programs. Aligned with federal goals, the VA Plan fosters regional collaboration to disburse risk, spread costs, and pool resources, thereby increasing overall return on investment. Private sector owners and operators are encouraged to participate in the National Infrastructure Protection Plan/ VA Plan partnership model and to initiate protective measures to augment existing plans for risk management, business continuity, as well as incident management, and emergency response. This National Preparedness Cycle will involve a continuous, mutually reinforcing, cycle of activity across four phases: Policy and Guidance, Planning and Resource Allocation, Training, Exercises and Lessons Learned, and Assessment and Reporting (Figure 4).

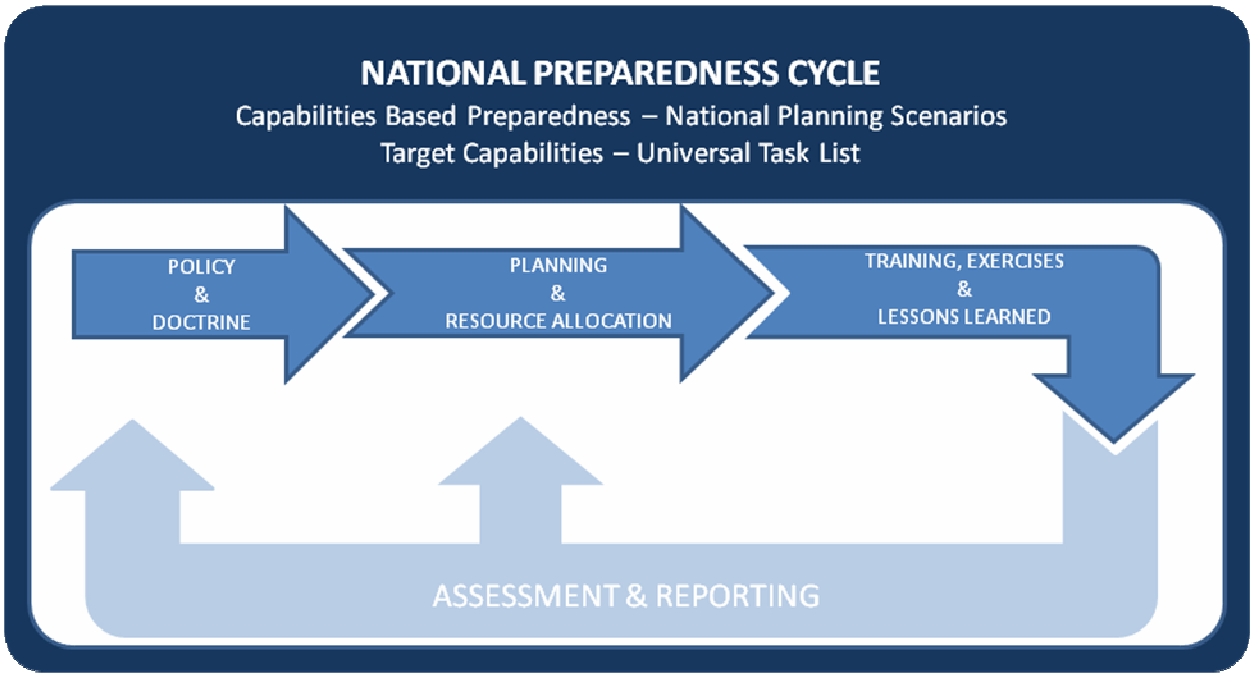

Figure 4 National Preparedness Cycle

1.3.1 Goals and Initiatives

The overarching goal of the *VA Plan* aligns with the vision of the Office of Commonwealth Preparedness (OCP): "to ensure a Virginia whose communities, businesses and government are safe, secure and prepared." To accomplish this, the OCP works with federal, state, and local officials, as well as the private sector, to develop a seamless, coordinated security and preparedness strategy and implementation plan.

Supporting goals include:

- Identification and protection of CIKR deemed most critical to the Commonwealth's public health and safety, governance, economic and physical security, and public confidence.
- Timely warning and assurance of the protection of those infrastructures and resources that face a specific, imminent threat.
- Pursuit of specific initiatives, enabling a collaborative environment in which federal, state, and local governments and the private sector can better protect, remediate, and recover the infrastructures and key assets they control following a disaster.
- Ensure sufficient funding is available to mitigate CIKR risks in the Commonwealth, to include pursuing federal funding under the DHS Grant Program, focusing existing state funding in a coordinated fashion consistent with this plan, and pursuing additional sources of funding to this effort such as General Fund allocations and other State appropriations.
- Integrate existing and future protective measures to identify, prioritize, and coordinate the Infrastructure Protection Program of CIKR within the Commonwealth.
- Understand, protect, and share information about terrorist threats and other hazards in a collaborative fashion among federal, state, local, and private sector stakeholders.
- Build security partnerships that will facilitate long-term risk management programs and maximize the efficient use of resources.

1.4 All-Hazards and CIKR Protection

Natural disasters can incur as much, if not more, destruction than a terrorist attack. Accordingly, CIKR protection initiatives should be viewed as complementary to traditional all-hazards planning.

1.5 Special Considerations

1.5.1 Protection of Information

It is imperative that information relevant to the protection of CIKR be safeguarded. The development of mutually beneficial, trusted relationships is of paramount importance, as any broad regulatory authority over CIKR does not exist, and the private sector cannot be compelled to submit infrastructure or regulatory information to the OCP. Further:

- Great care must be taken by the government to ensure that sensitive infrastructure information is protected and used appropriately to enhance the protection of the Commonwealth's CIKR;
- Information on specific industry assets and vulnerabilities is particularly sensitive because public release may lead to breaches in security, competitive advantage, and/or adverse impacts on an industry's position in the marketplace.

1.5.2 The Cyber Dimension

The Virginia Information Technologies Agency is the Commonwealth's consolidated, centralized information technology organization.

The delicate nature of cyber networks and information is self-evident. Reducing cyber risk and enhancing cyber security should be addressed in two ways:

- As a cross-sector cyber element that involves the OCP, the Virginia Information Technologies Agency, the Sector Specific Agencies, and private sector owners and operators; and
- As a major component of the Information Technology sector's responsibility in partnership with the Telecommunications Sector.

1.5.3 The Human Element

Assessing human element vulnerabilities is more subjective than assessing the physical or cyber vulnerabilities of corresponding assets, systems, and networks. The human element requires additional consideration of workforce availability and reliability in the face of post modern terrorist threats, such as chemical or biological attacks. Even naturally occurring illnesses, such as Pandemic Influenza, could necessitate the ability of employees to work from alternate locations. The assessment of the human element in this case and in related business continuity issues is extremely challenging, but necessary.

Other requirements include:

- Identifying and preventing the insider threat resulting from infiltration or individual employees determined to do harm;
- Identifying, protecting, and cross-training employees with critical knowledge; and
- Identifying and mitigating fear tactics used by terrorist agents and disaffected insiders;
- Diverse protective programs and actions, such as background checking and establishing methods of personnel surety, to address threats posed by employees and to employees need to be implemented across all sectors.

1.6 Achieving the Goal of the VA Plan

The following are considered measures of success in implementing the *VA Plan*:

- Coordinated, risk-based CIKR plans and programs in place addressing known and potential threats, and hazards;
- Structures and processes that are flexible and adaptable to incorporate operational lessons learned and best practices, as well as to quickly adjust to a changing threat or incident environment;
- Processes in place to identify and address dependencies and interdependencies to allow for more timely and effective implementation of short-term protective actions and more rapid response and recovery; and

- Access to robust information-sharing networks that include relevant intelligence and threat analysis, and real-time incident reporting.

1.6.1 Building Security Partnerships

Building security partnerships represents the foundation of the Commonwealth's CIKR protection effort. These partnerships provide a framework to:

- Exchange ideas, approaches, and best practices;
- Facilitate security planning and resource allocation;
- Establish effective coordination among security partners;
- Enhance coordination with the interstate community; and
- Build public awareness.

CHAPTER 2 AUTHORITIES, ROLES, AND RESPONSIBILITIES

Improving the protection of the Commonwealth's CIKR in an all-hazards environment requires a comprehensive, unifying organization; clearly defined roles and responsibilities; and close cooperation across all levels of government and the private sector. Protection authorities, requirements, resources, capacities, and risk landscapes vary widely across governmental jurisdictions, sectors, as well as individual industries and enterprises. This reality presents a complex set of challenges in terms of *VA Plan* compliance and performance measurement. With the obligation to protect the citizens and infrastructure of the Commonwealth as a primary duty, Governor Kaine has promulgated Executive Order 44 (2007) which establishes preparedness initiatives within the Commonwealth and requires all executive branch agencies to include emergency preparedness planning as a core component of their mission.

Sector-Specific Plans will support continued refinement of Agency emergency preparedness plans. Hence, successful implementation of the *VA Plan* depends on an effective partnership framework that fosters integrated, collaborative engagement and interaction, establishes a clear division of responsibilities among diverse federal, state, regional, local, and private sector security partners, and efficiently allocates the Commonwealth's protection resources based on risk and need. The *VA Plan* will be reviewed and updated annually by the appropriate Secretariats, with the concurrence of OCP.

2.1 Authorities

The roles and responsibilities described in this Chapter are derived from a series of federal and Commonwealth authorities, including Executive Order 44, other CIKR protection-related legislation, executive orders, and Gubernatorial strategies. Executive Order 44, § 44-146.17 of the Code of Virginia are the primary authority for the Commonwealth's overall homeland security mission.

The Commonwealth strategy for protection and resiliency establishes a CIKR vision to ensure a safe, secure, and prepared Virginia by developing and overseeing a coordinated prevention, preparedness, response, and recovery strategy for natural and man-made disasters, and emergencies.

2.2 Roles and Responsibilities

Given that terrorist attacks and certain natural or manmade disasters can have an impact across Virginia and its neighboring states, it is incumbent upon the Commonwealth to provide overarching leadership and coordination in the CIKR protection and resiliency mission area. Figure 5 depicts the organizational structure of the Commonwealth with regard to CIKR preparedness.

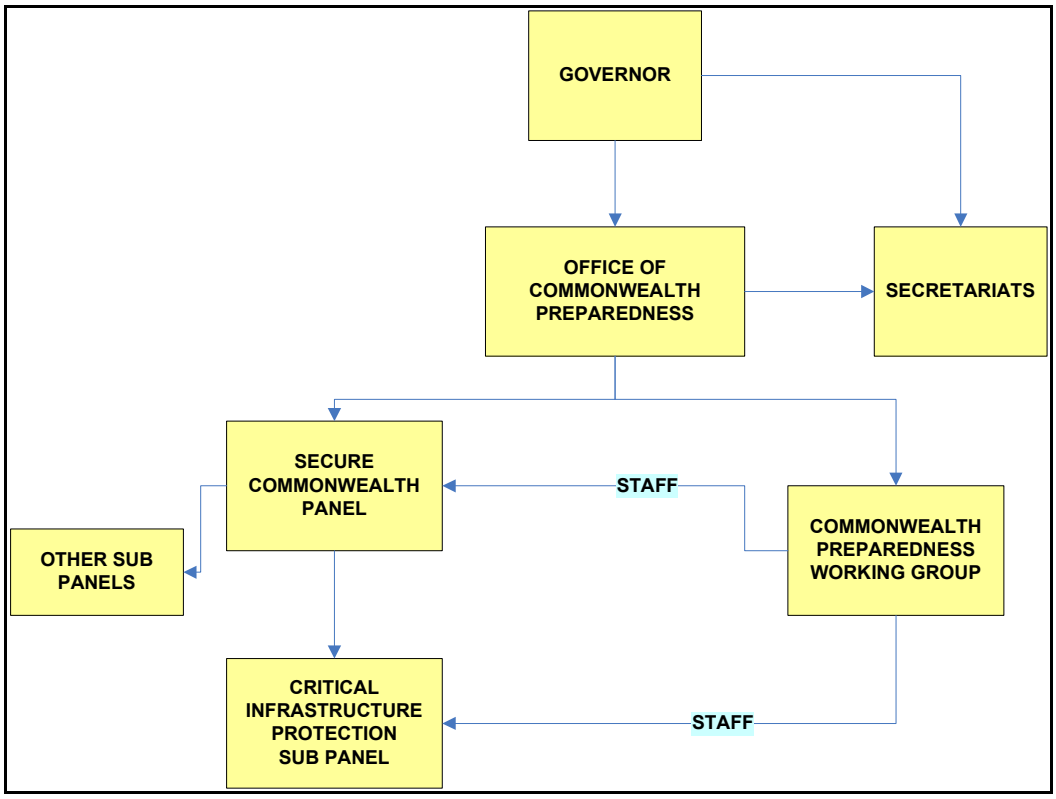

Figure 5. Commonwealth Decision-Making Process

2.2.1 State Sector-Specific Agencies

Recognizing that each CIKR sector possesses its own unique characteristics, operating models, and risk landscape, the Commonwealth has designated state secretariats and agencies for each of the CIKR Sectors. OCP will provide assistance to State Sector Specific Agencies in the completion of their Sector-Specific Plans. Sector Specific Agencies are responsible for working to implement the *VA Plan* sector partnership model and risk management framework, develop protective programs and related requirements, and provide sector-level CIKR protection guidance.

State Sector Specific Agencies are also responsible for collaborating with private sector security partners and encouraging the development of appropriate information-sharing mechanisms within the sector. This includes supporting sector coordinating committees to facilitate sharing of information on physical and cyber threats, vulnerabilities, incidents, recommended protective measures, and security-related best practices. This also includes encouraging voluntary security-related information sharing, where possible, among private entities within the sector, as well as among public and private entities.

State Sector Specific Agencies perform the activities, as appropriate and consistent with existing authorities (including regulatory authorities in some instances), in close cooperation with other security partners. Refer to Figure 10 in Appendix A for a breakdown of State Sector Specific Agencies and their areas of responsibility.

Additional State Sector-Specific Agency responsibilities include:

- Identifying, prioritizing, and coordinating the protection of sector-level CIKR with a particular focus on CIKR that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a WMD;
- Managing the overall process for building security partnerships and leveraging CIKR security expertise, relationships, and resources within the sector;
- Coordinating, facilitating, and supporting comprehensive risk assessment/management programs for high-risk CIKR, identifying protection priorities, and incorporating CIKR protection activities as a key component of the all-hazards approach to domestic incident management within the sector;
- Facilitating the sharing of real-time incident notification, as well as CIKR protection best practices and processes, and risk assessment methodologies and tools within the sector;
- Promoting sector-level CIKR protection education, training, and awareness in coordination with state, regional, local, and private sector partners;
- Monitoring performance measures for sector-level CIKR protection and VA Plan implementation activities to enable continuous improvement, and reporting progress, and gaps to the OCP;
- Identifying/recommending appropriate strategies to encourage private sector participation;
- Supporting protocols for the Protected Critical Infrastructure Information Program;
- Working with the OCP to develop, evaluate, validate, or modify sector-specific risk assessment tools;
- Supporting sector-level dependency, interdependency, consequence, and other analysis as required;
- Coordinating sector-level participation in the Commonwealth Exercise Program and other sector-level activities; and

- Supporting the OCP in efforts to coordinate Virginia CIKR protection programs regionally and with DHS.
- Identifying CIKR sites and/or facilities and reporting same to OCP for inclusion into the Virginia CIKR database.
- Assist sector security partners in their efforts to apply above methodology and plans in their respective organizations.

2.2.2 Supporting Commonwealth Entities to Sector-Specific Agencies

All Commonwealth agencies, offices, and entities, function as security partners in coordination with OCP and the State Sector Specific Agencies, for example the Virginia Department of Emergency Management (VDEM), Virginia Department of Transportation (VDOT) Critical Infrastructure Protection and the Virginia State Police. In this capacity, they support implementation of the *VA Plan* and Sector-Specific Plans, as appropriate, and are responsible for identification, prioritization, assessment, remediation, and enhancing the protection of CIKR under their control. Additionally, the OCP will lead in the development of Vulnerability Assessment Teams, whose members will be subject matter experts drawn from State, Local and Private Sector entities. The Vulnerability Assessment Teams will support all Sector Specific Agencies in developing their Sector-Specific Plans.

Commonwealth elements that are not designated as Sector Specific Agencies, but have unique responsibilities, functions, or expertise in a particular CIKR sector will support Sector Specific Agencies in the development of their Sector-Specific Plans.

2.2.2.1 Virginia Fusion Center

The coordination of information and resources from key critical response elements is fundamental in providing a well orchestrated and coordinated response to homeland security events affecting the Commonwealth. The Virginia Fusion Center, created to improve Commonwealth preparedness and resiliency against terrorist attacks, maintains and monitors access to a number of databases and resources. The Virginia Fusion Center is a valuable resource available to Sector Specific Agencies in support of their Sector-Specific Plans.

2.2.2.2 Virginia Department of Military Affairs

The National Guard is the lead military agency for homeland security in the Commonwealth of Virginia. The Guard's primary missions are integration with the military in the context of national security and serving as a protection and response force, for the Governor, in dealing with domestic emergencies. The Virginia National Guard will collaborate with OCP managed preparedness, protection, and resiliency initiatives (such as Critical Infrastructure Protection and Vulnerability Assessment Teams) to support the Commonwealth.

2.2.3 Local Governments

Local governments are the front line of preparedness and resiliency in the homeland security mission. They play a direct role in enabling the protection of the Commonwealth's CIKR, and more specifically, they are responsible for the implementation of the *VA Plan*. They act as a focal point for and promoting the

coordination of protective and emergency response activities, preparedness programs, and resource support within their jurisdictions. They provide critical public services and functions in conjunction with private sector owners and operators. Local governments are critical partners under the *VA Plan* framework. They drive emergency preparedness, as well as local participation in the *VA Plan* implementation across a variety of jurisdictional security partners; including government agencies, CIKR owners and operators, and private citizens in the communities they serve. Figure 6 depicts local interaction in the development of a Sector-Specific Plan.

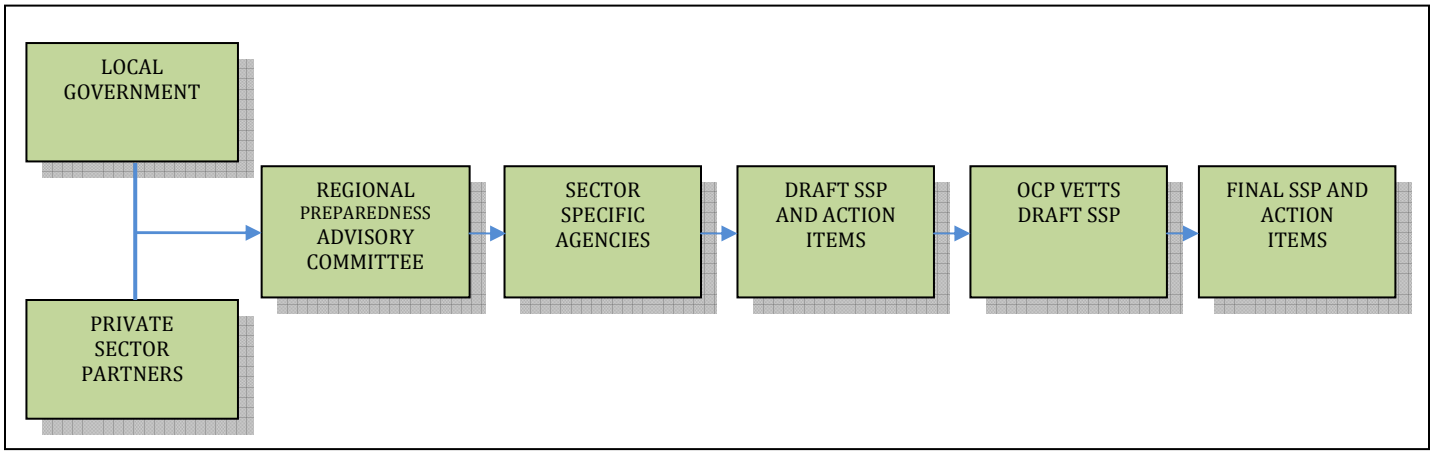

Figure 6. Local Government Interaction in Sector-Specific Plan Development

CIKR protection focus at the local level should include, but is not limited to:

- Acting as a focal point for and promoting the coordination of protective and emergency response activities, preparedness programs, and resource support among local agencies, businesses, and citizens;
- Developing a unified approach at the local level for CIKR identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant security partners within the jurisdiction;
- Identifying, implementing, and monitoring a risk management plan, and taking corrective actions as appropriate;
- Participating in significant national, regional, and local awareness programs to encourage appropriate management and security of cyber systems;
- Facilitating the exchange of security information, including threat assessments, attack indications and warnings, and advisories, among security partners within the jurisdiction;
- Addressing unique geographical issues (including trans-border concerns) dependencies, and interdependencies among agencies and enterprises within the jurisdiction;

- Identifying and implementing plans and processes for increases in protective measures that align to all-hazards warnings, specific threat vectors as appropriate, and each level of the Homeland Security Advisory System; and
- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents, and applying that learning, where applicable, to the CIKR protection context.

2.2.4 Private Sector Owners and Operators

Owners and operators generally represent the first line of defense for the CIKR under their control. Private sector owners and operators are responsible for taking action to support risk management planning and investments in security as a necessary component of prudent business planning and operations. In today's risk environment, these activities generally include reassessing and adjusting continuity-of-business and emergency management plans, building increased resiliency and redundancy into business processes and systems, protecting facilities against physical and cyber attacks and natural disasters, guarding against the insider threat, and increasing coordination with external organizations to avoid or minimize the impacts on surrounding communities or other industry partners.

2.2.5 Regional Partners

Additional regional partnerships within the Commonwealth are supported by the National Capitol Region, Richmond Area and Hampton Roads Region initiatives. These initiatives are directed to oversee and coordinate federal programs for state, local, and regional authorities in these areas.

2.2.6 Boards, Commissions, Authorities, Councils, and Other Entities

These groups include, but are not limited to: transportation authorities, public utility commissions, water and sewer boards, park commissions, housing authorities, public health agencies, and many others. These entities may serve as State Sector Specific Agencies within the Commonwealth and contribute expertise, assist with regulatory authorities, or help to facilitate investment decisions related to CIKR protection efforts within a given jurisdiction or geographical region.

2.2.6.1 Secure Commonwealth Panel

The Secure Commonwealth Panel (SCP) is established as an advisory board in the executive branch of State government.

2.2.6.2 Commonwealth Preparedness Working Group

The Commonwealth Preparedness Working Group (CPWG) consists of cross-secretariat, state agency, and sector-specific partners who coordinate, develop, and implement policy on funding and operational issues relating to all-hazards preparedness.

2.2.6.3 Virginia Military Advisory Council

The Virginia Military Advisory Council (VMAC) was established to maintain a cooperative and constructive relationship between the Commonwealth and the leadership of the Armed Forces of the United States, located within the Commonwealth.

CHAPTER 3 THE PROTECTION PROGRAM STRATEGY: MANAGING RISK

The cornerstone of the *VA Plan* is its risk management framework. Risk is generally defined as the combination of the frequency of occurrence, vulnerability, and the consequence of a specified hazardous event. In the context of the *VA Plan*, risk is the expected magnitude of loss (e.g., deaths, injuries, economic damage, loss of public confidence, or government capability) due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss. The VA Plan risk management framework (Figure 7) establishes the process for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of Commonwealth or sector-specific risk that drives CIKR protection activities. In Virginia, OCP is responsible for overall state risk-based CIKR prioritization in close collaboration with Virginia Sector Specific Agencies and other security partners.

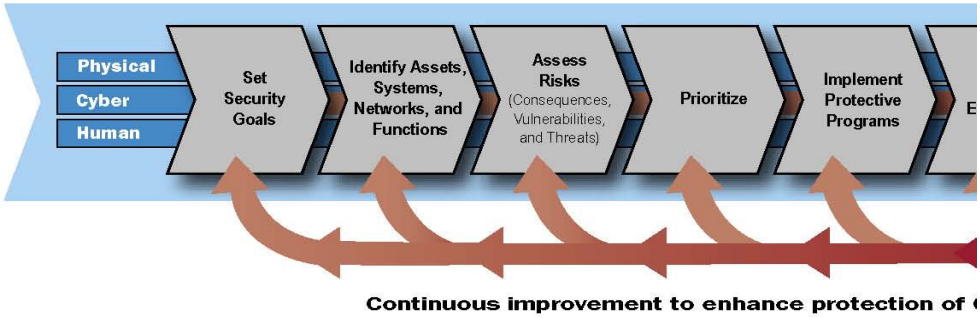

Figure 7. Risk Management Framework

The framework applies to the general threat environment, as well as to specific threats or incident situations. The risk management framework is tailored and applied on an asset, system, network, or function basis, depending on the fundamental characteristics of the individual CIKR sectors. For those sectors primarily dependent on fixed assets and physical facilities, a bottom-up, asset-by-asset, approach may be most appropriate. For sectors with diverse physical and virtual assets, such as Telecommunications and Information Technology, a top-down, business, or mission continuity approach that focuses on networks, systems, and functions may be more effective. Each sector chooses the approach that produces the most actionable results for the sector and works to ensure that the relevant risk analysis procedures are compatible with the criteria established in the *National Infrastructure Protection Plan*.

The *VA Plan* risk management framework includes the following activities:

- Set security goals: Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.
- Identify assets, systems, networks, and functions: Develop an inventory of the

assets, systems, and networks (including those located outside the Commonwealth of Virginia) that compose the Commonwealth's CIKR and the critical functionality therein; collect information pertinent to risk management that takes into account the fundamental characteristics of each sector.

- Assess risks: Determine risk by using standard risk assessment methodology combining potential direct and indirect consequences from an all-hazards approach (including seasonal changes in consequences, and dependencies and interdependencies associated with each identified asset, system, or network), known vulnerabilities to various potential attack vectors, and general or specific threat information.
- Prioritize: Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk; establish priorities based on risk; and determine protection and business continuity initiatives that provide the greatest mitigation of risk.
- Implement protective programs: Select sector-appropriate protective actions or programs to reduce or manage the risk identified; secure the resources needed to address priorities.
- Measure effectiveness: Use metrics and other evaluation procedures at the state and sector levels to measure progress and assess the effectiveness of the CIKR protection program in improving protection, managing risk, and increasing resiliency.

A complete explanation of the Risk Management Framework can be found in Chapter 3 of the National Infrastructure Protection Plan:

http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

3.1 Performance Measures Relevant to Virginia

Metrics are required to analyze the performance of ongoing and future CIKR protection and resiliency initiatives. The State Sector Specific Agencies will develop, with OCP guidance, and in a collaborative process that includes State Sector Specific Agencies and other private sector security partners, metrics that are tailored to the unique characteristics of each sector and are used to assist in monitoring progress within a specific sector. Essentially, the above will provide the framework for assessing the efficacy of the Sector-Specific Plans.

Special emphasis must be placed on allocating resources to support a safe Commonwealth. The near infinite demands of effective protection and resiliency and limited resources available to meet these demands, require grant programs that allocate resources according to where they will be most effective. There are a number of Federal and Commonwealth grant initiatives designed to support protection and resiliency in the Commonwealth.

Chapter 4 ORGANIZING AND PARTNERING FOR CIKR

Protection

The diversity and complexity of the Commonwealth's CIKR, the distributed character of its associated protective architecture, and the uncertain nature of manmade or natural disasters make the effective implementation of protection efforts a great challenge. To be effective, the *VA Plan* will be implemented using organizational structures and partnerships committed to sharing and protecting the information needed to achieve the goal of the *VA Plan*.

4.1 Leadership and Coordination Mechanisms

4.1.1 National-Level Coordination

The DHS Office of Infrastructure Protection facilitates overall development of the *National Infrastructure Protection Plan* from which the *VA Plan* is derived. The Office of Infrastructure Protection coordinates resource distribution through the Office of Grants and Training via the State Administrative Agency (SAA) (Virginia Department of Emergency Management).

4.1.2 Commonwealth Coordination

The OCP (in cooperation with SAA) facilitates overall development of the *VA Plan* and State Sector-Specific Plans, provides overarching guidance monitors the full range of associated coordination activities and performance metrics, and ensures Commonwealth plans and programs correlate with the *National Infrastructure Protection Plan*. Additionally the OCP:

- Chairs VA Plan Coordinating Council comprised of designated Sector Leads and others as appointed;
- Facilitates the *VA Plan* revisions and updates using a comprehensive Commonwealth review process;
- Ensures that effective policies, approaches, guidelines, and methodologies regarding partner coordination are developed and disseminated to enable State Sector Specific Agencies and other security partners to carry out the *VA Plan* responsibilities;
- Facilitates the sharing of CIKR protection-related best practices and lessons learned;
- Facilitates security partner participation in preparedness activities, planning, readiness exercises, and public awareness efforts; and
- Ensures cross-sector coordination of Sector-Specific Plans to avoid duplicative requirements and reporting, and conflicting guidance.

4.1.3 Regional Coordination

Regional partnerships, groupings, and governance bodies enable CIKR protection coordination among security partners like the Regional Preparedness Advisory Committees (RPAC).

4.1.4 Sector Coordination

The *VA Plan* relies on the sector partnership model, as the primary organizational structure for coordinating CIKR efforts and activities. The sector partnership model encourages formation of Sector Coordinating Committees. OCP provides Sector Specific Agencies with guidance in establishing these committees, and tools, and support to enable these groups to work together to carry out their respective roles and responsibilities. Sector Coordinating Committees work to create a coordinated framework for CIKR protection within and across sectors.

The sector partnership model encourages participation by CIKR owners and operators in the creation and sustainment of Sector Coordinating Committees. These committees serve as the principal entity for coordinating with the Commonwealth on a wide range of CIKR protection activities and issues. Sector Coordinating Committees should be individually organized, self-run, and self-governed, with a spokesperson designated by the sector membership. The Sector Coordinating Committees enable CIKR owners and operators to interact on a wide range of sector-specific strategies, policies, activities, and issues. The primary functions of a Sector Coordinating Committee include the following:

- Represent a primary coordination point with government in the sector for addressing the entire range of CIKR protection activities and issues for that sector;
- Serve as a strategic communications and coordination mechanism between CIKR owners, operators, and suppliers, and with the government during response and recovery as determined by the sector;
- Identify, implement, and support the information-sharing capabilities and mechanisms that are most appropriate for the sector. Information Sharing and Analysis Centers (ISAC) may perform this role if so designated by the Sector Coordinating Committee;
- Facilitate inclusive organization and coordination of the sector's policy development regarding CIKR protection planning and preparedness, exercises and training, public awareness, and associated plan implementation activities and requirements;
- Advise on integration of federal, state, regional, and local planning with private sector initiatives;
- Provide input to the government on sector research and development (R&D) efforts and requirements; and
- Sector Coordinating Committees are encouraged to participate in voluntary development efforts to ensure that sector perspectives are included in standards that affect CIKR protection.

4.2 Protection of Sensitive CIKR Information

The *VA Plan* implementation will rely greatly on critical infrastructure information provided by the private sector. Much of this is sensitive business or security information

that could cause serious damage to companies, the economy, and public safety, or security through unauthorized disclosure or access to this information.

The Federal Government and the Commonwealth of Virginia have a statutory responsibility to safeguard information collected from or about CIKR activities. Section 201(d)(12)(a) of the Homeland Security Act requires DHS to "ensure that any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties." DHS and other Federal agencies use a number of programs and procedures, such as the Protected Critical Infrastructure Information Program, to ensure that CIKR information is properly safeguarded.

4.2.1 Protected Critical Infrastructure Information Program

The Commonwealth of Virginia earned DHS Protected Critical Infrastructure Information Program accreditation in 2007. The program provides a means for sharing private sector information with the government while providing assurances that the information will be exempt from public disclosure and will be properly safeguarded. This enables members of the private sector to voluntarily submit sensitive information regarding CIKR to the Commonwealth and DHS with the assurance that the information will be protected.

4.2.1.1 Protected Critical Infrastructure Information Program Office

The Commonwealth Protected Critical Infrastructure Information Officer is responsible for managing Protected Critical Infrastructure Information program compliance, training of authorized users, and maintenance of Standard Operating Procedures in Virginia.

4.2.1.2 Critical Infrastructure Information Protection

The following process and procedures apply to all Critical Infrastructure Information submissions:

- Individuals or collaborative groups may submit information for protection;
- The DHS Protected Critical Infrastructure Information Program Office validates that the information qualifies for protection under the act;
- All validated Protected Critical Infrastructure Information is stored in a secure data management system and security partners follow DHS sharing guidelines for unclassified but sensitive information;
- Secure methods are used for disseminating Protected Critical Infrastructure Information; and
- Authorized users must comply with safeguarding requirements defined by the DHS Protected Critical Infrastructure Information Program Office.

4.2.1.3 Uses of Protected Critical Infrastructure Information

Protected Critical Infrastructure Information may be shared with authorized government entities, including Federal, State, or local government employees or contractors supporting governmental agencies, only for the purposes of securing CIKR and protected systems. Protected Critical Infrastructure Information will be used for

analysis, prevention, response, recovery, or reconstitution of CIKR threatened by terrorism or other hazards.

Authorized government entities may generate advisories, alerts, and warnings relevant to the private sector based on the information provided; however, communications made available to the public will not contain any sensitive information provided by the submitter. Protected Critical Infrastructure Information can be combined with other information, including classified information, in support of CIKR protection activities; in such cases, Protected Critical Infrastructure Information used in such products must be marked accordingly.

4.2.1.4 Protected Critical Infrastructure Information Protections and Authorized Users

The Protected Critical Infrastructure Information Program has established procedures to ensure that Protected Critical Infrastructure Information is properly accessed, used, and safeguarded throughout its life cycle.

4.2.2.5 Physical and Cyber Security Measures

OCP and Sector Specific Agencies will use strict information security protocols for the access, use, and storage of sensitive information (including that related to CIKR). These protocols include both physical security measures and cyber security measures equivalent to those employed by DHS.

4.3 Privacy and Constitutional Freedoms

Directives outlined in the *VA Plan* are intended to provide a balance between achieving a high level of security and protecting the civil rights and liberties that form an integral part of America's national character and the expectations of the citizens of the Commonwealth of Virginia. Achieving this balance requires acceptance of some level of risk. In providing for effective protective programs, the processes outlined in the *VA Plan* respects privacy, freedom of expression, freedom of movement, freedom from unlawful discrimination, and other liberties that define the American way of life. Compliance with the Privacy Act and governmental privacy regulations and procedures is a key factor that is considered when collecting, maintaining, using, and disseminating personal information.

Chapter 5 INTEGRATING CIKR PROTECTION AS PART OF THE COMMONWEALTH PREPAREDNESS MISSION

5.1 A Coordinated National Approach to the Homeland Security Mission

The *VA Plan* provides the coordination and collaboration structure needed to integrate and synchronize activities derived from various relevant statutes, Governor Executive Orders, regional and national strategies, and Presidential Directives. The relevant authorities include those that address the overarching homeland security and CIKR protection missions, as well as those that address a wide range of sector-specific CIKR protection-related functions, programs, and responsibilities.

It is imperative that all levels of government and the private sector cooperate closely to provide effective and efficient CIKR protection. This section describes how overarching homeland security legislation, strategies, Homeland Security Presidential Directives (HSPD), State, and private sector initiatives are combined to provide CIKR protection. Information regarding sector-specific CIKR-related authorities will be addressed in the Sector-Specific Plans as they are developed.

5.1.1 Legislation

The Homeland Security Act provides the primary authority for the overall homeland security mission and establishes the basis for the *National Infrastructure Protection Plan*, the Sector-Specific Plans, and related CIKR protection efforts (Figure 8).

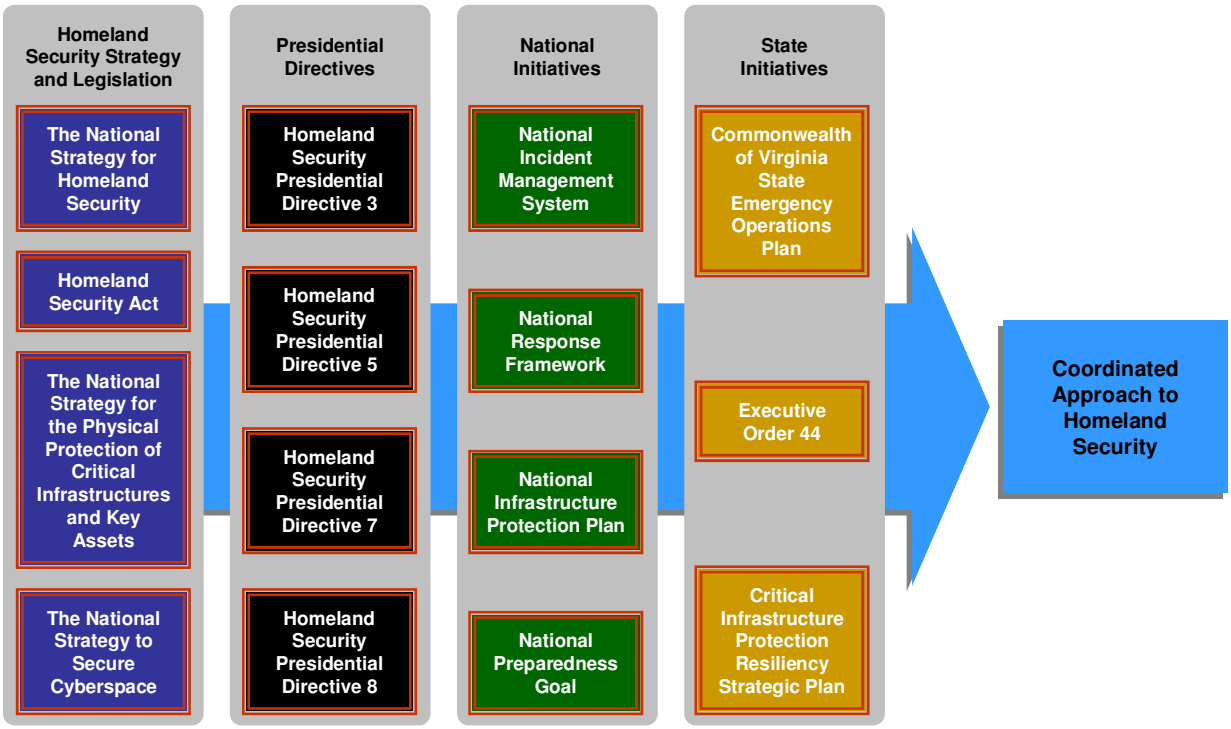

Figure 8. National Framework for Homeland Security

5.2 Relationship of the National Infrastructure Protection Plan *and Sector-Specific Plans to State, Regional and Local CIKR Protection Programs*

At the Federal government level, the National Incident Management System (NIMS), the National Response Framework and the *National Infrastructure Protection Plan* are complementary plans. The National Incident Management System and National Response Framework address emergency management, emergency planning, and incident management in general at the national level. The *National Infrastructure Protection Plan* specifically addresses the protection of CIKR. All three are complementary and provide the overarching plans for homeland security.

The last column in Figure 8 contains Commonwealth of Virginia Directives and Initiatives. These are the State Emergency Operations Plan, Executive Order 44 (2007), and this document, the *Virginia Critical Infrastructure Protection & Resiliency Strategic Plan*. While the first two documents refer to emergency management and emergency planning in general, the *VA Plan* addresses the issue of CIKR specifically. Nonetheless, all three complement each other and serve to enhance the Commonwealth's overall preparedness.

5.2.1 Sector-Specific Plans

Based on guidance from the OCP, Sector-Specific Plans are developed jointly by State Sector Specific Agencies in close collaboration with Sector Coordinating Committees and others including State and local homeland security partners with key interest or expertise appropriate to the sector. Sector-Specific Plans are tailored to address unique characteristics and risk landscapes of each sector while also providing consistency for protective programs. Sector-Specific Plan functions can be found in Chapter 5 of the *National Infrastructure Protection Plan:* (http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

The structure of the Sector-Specific Plans is shown in Figure 9.

Executive Summary
Introduction
1. Sector Profile and Goals
2. Identify Assets, Systems, Networks, and Functions
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs
6. Measure Progress
7. CIKR protection R&D
8. Sector Management and Coordination Appendices

Figure 9. Structure of Sector-Specific Plans

Refer to Appendix A for more detail.

An initial draft of the Sector-Specific Plans must be completed and submitted by the State Sector Specific Agencies to the Office of Commonwealth Preparedness within 180 days of issuance of the *VA Plan*. Acceptance of the Sector-Specific Plan will be the decision of the OCP. The OCP will provide guidance and oversight to support the State Sector Specific Agencies completion of their Sector-Specific Plans.

5.3 CIKR Protection and Incident Management

5.3.1 The National Response Framework

The National Response Framework provides an all-hazards approach to a wide array of natural disasters, terrorist threats and incidents, and other emergencies. Federal Sector Specific Agencies have roles within the National Response Framework structure that are distinct from, yet complementary to, their responsibilities under the *National Infrastructure Protection Plan*. Likewise State Sector Specific Agency responsibilities' under the *VA Plan* reflect Federal Sector-Specific Agency responsibility under the *National Infrastructure Protection Plan*.

5.3.2 Transitioning From *National Infrastructure Protection Plan* Steady-State to Incident Management

A variety of alert and warning systems that exist for natural hazards, technological or industrial accidents, and terrorist incidents provide the bridge between routine steady-state operations using the *National Infrastructure Protection Plan* risk management framework and incident management activities using the National Response Framework /National Incident Management System concept of operations for actions related to both pre-incident prevention and post-incident response and recovery (e.g., hurricane and tornado warnings).

In transitioning from steady-state processes to National Response Framework /State EOC incident management coordination includes the following actions by the OCP, Virginia Department of Emergency Management, Virginia State Police, State Sector Specific Agencies and other security partners should consider:

- Increasing protection levels to correspond with the threat through the Homeland Security Advisory System or other relevant all-hazards alert and warning systems;
- Using information-sharing networks;
- Facilitating communications between security partners;
- Fulfilling roles as defined in the National Response Framework /State EOC for incident management activities; and
- Working with sector-level information sharing entities.

CHAPTER 6 ENSURING AN EFFECTIVE AND EFFICIENT PROGRAM OVER THE LONG TERM

This chapter addresses the efforts needed to ensure an effective, efficient, CIKR protection program over the long term. It focuses particularly on the long-lead-time elements of CIKR protection that require sustained plans and investments over time, such as generating skilled human capital, developing high-tech systems, and building public awareness.

Key activities needed to enhance CIKR protection over the long term include:

- Building awareness across Virginia to support the CIKR protection program, related protection investments, and protection activities by ensuring a focused understanding of the all-hazards threat environment and of what is being done to protect and enable the timely restoration of CIKR in light of such threats;
- Enabling education, training, and exercise programs to ensure that there are skilled and knowledgeable professionals and experienced organizations are able to undertake *VA Plan* related responsibilities in the future;
- Continuously improving the *VA Plan* and associated plans and programs through ongoing management and revision, as required.
- Supporting R&D and using technology to improve protective capabilities or to lower the costs of existing capabilities so that security partners can afford to do more with limited budgets;

6.1 Continuously Improving the *Virginia Plan* and the *Sector-Specific Plans*

The *VA Plan* through the responsible Sector Specific Agencies use, local government and Private Sector Cross-Sector Councils as the primary forums for coordination of policy, planning, training, and other requirements needed to ensure efficient implementation, and ongoing management and maintenance of the *VA Plan,* and the Sector-Specific Plans.

6.1.1 Management and Coordination

The OCP is the executive agent for *VA Plan* management and maintenance.

The *VA Plan* is a multi-year plan describing mechanisms for sustaining the Commonwealth's preparedness and resiliency. The *VA Plan* and its component Sector-Specific Plans include a process for annual review; periodic interim updates as required; and regularly scheduled partial reviews and re-issuance every 3 years, or more frequently, if directed by the OCP. The OCP will oversee the review and maintenance process for the *VA Plan.* The State Sector Specific Agencies, in coordination with the Sector Coordinating Committees, will establish and operate the mechanism(s) necessary to coordinate this review for their respective Sector-Specific Plans. The *VA Plan* and Sector-Specific Plan revision processes will include developing or updating any documents necessary to carry out preparedness and resiliency activities. At a minimum, the VA Plan will be reviewed annually. As changes are warranted, updates to the VA Plan will be issued.

6.1.2 Maintenance and Updating

The following paragraphs establish the procedures for posting interim changes and periodic updating of the *VA Plan*:

- Types of Changes: Changes include additions of new or supplementary material and deletions. No proposed change should contradict or override authorities or other plans contained in statute, executive order, or regulation.
- Coordination and Approval: While the OCP is the Governor's executive agent for

the *VA Plan* management and maintenance, any Commonwealth department, agency, or entity with assigned responsibilities under the *VA Plan* may propose a change to the plan. The OCP is responsible for coordinating the review and approval of all proposed modifications to the *VA Plan* with State Sector Specific Agencies and other security partners, as appropriate. Policy changes will be coordinated and approved through the process dictated by the OCP.

- Notice of Change: The OCP will issue an official Notice of Change for each interim revision to the *VA Plan*. After publication, the modifications will be considered part of the *VA Plan* for operational purposes pending a formal revision and re-issuance of the entire document. Interim changes can be further modified or updated using this process.
- Distribution: The OCP will distribute Notices of Change to State Sector Specific Agencies, and other security partners. Notices of Change to other organizations will be provided upon request.
- Re-Issuance: At a minimum the OCP will coordinate reviews and updating of the *VA Plan* annually, with occuring revisions every 3-years. The review and updating will consider lessons learned and best practices identified during implementation in each sector and will incorporate the periodic changes and any new information technologies. The OCP will distribute revised *VA Plan* documents for interagency review and concurrence through the appropriate process.

The State Sector Specific Agencies, in coordination with the Sector Coordinating Committees, will establish and operate the mechanism(s) necessary to coordinate Sector-Specific Plan maintenance and updates in accordance with the above guidelines. Ensuring an effective, efficient, program over the long term requires dedicated resources and the adoption of a culture of preparedness throughout all of the critical infrastructure partners both public and private.

CHAPTER 7 PROVIDING RESOURCES FOR THE CIKR PROTECTION PROGRAM

7.1 The Risk-Based Resource Allocation Process

Critical Infrastructure and Key Resource protection is funded on the basis of resources directed to areas of greatest priority for effective risk management. Using a risk-based approach, the Commonwealth, in conjunction with other relevant parties, identifies those assets, systems, etc. that are most critical to the state and the nation.

7.1.1 Sector-Specific Agency Reporting to the Office of Commonwealth Preparedness

The first step for a State Sector Specific Agency in the risk-based allocation process is to coordinate with sector partners, including Sector Coordinating Committees as appropriate, to accurately determine sector priorities, program requirements, and funding needs for CIKR protection. The OCP will provide State Sector Specific Agencies

with reporting guidance and templates that include requests for specific information, such as CIKR protection priorities, requirements, and resources. Annual Reports from all sources will be due the 1st of July each calendar year. The following should be included in the Sector CIKR Protection Annual Report to assist in prioritization of funds:

- Priorities and annual goals for CIKR protection and associated gaps;
- Sector-specific requirements for CIKR protection activities and programs based on risk and need; and
- Projected CIKR-related resource requirements for the sector, with an emphasis on anticipated gaps or shortfalls in funding for sector-level CIKR protection and/ or for protection efforts related to national-level CIKR that exist within the sector.

APPENDIX A:

COMMONWEALTH SECTOR-SPECIFIC PLANS

A.1 Overview of State Sector-Specific Plans

The *VA Plan* provides the coordinated approach that will be used to establish State priorities, goals, and requirements for Critical Infrastructure (CI) and Key Resource (KR) protection. This coordinated approach will allow Federal and State funding and resources to be applied in the most effective manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents. The *VA Plan*, in alignment with the Department of Homeland Security (DHS) National Infrastructure Protection Plan, establishes overarching concepts relevant to all CIKR sectors identified in Homeland Security Presidential Directive 7 and establishes preparedness initiatives within the Commonwealth directed in Governor Kaine's Executive Order 44 (2007). Figure 10 shows what Commonwealth Secretariats and Sector-Specific Agencies are assigned to each CIKR sector.

(* Designates LEAD AGENCY)

Critical Infrastructure/Key Resources Sector	Secretariats	Virginia's Sector Specific Agencies (As assigned by OCP)
Agriculture and Food	Agriculture and Forestry	* Department of Agriculture and Consumer Services Department of Health
Defense Industrial Base	Public Safety Transportation	* Department of Military Affairs
Energy	Natural Resources	* Department of Mines, Minerals and Energy State Corporation Commission
Public Health and Healthcare	Health and Human Resources	* VA Department of Health Department of Environmental Quality
National/State Monuments and Icons	Natural Resources	* Department of Conservation and Recreation Virginia Tourism Corporation Department of Historic Resources State Council of Higher Education for Virginia
Banking and Finance	Finance	* Department of the Treasury State Corporation Commission

Drinking Water and Water Treatment Systems	Health and Human Resources	* Department of Health Department of Environmental Quality
Chemical	Health and Human Resources	* Department of Environmental Quality Department of Health Department of Emergency Management Department of Agriculture and Consumer Services Department of State Police
Commercial Facilities	Commerce and Trade	* Department of Business Assistance Virginia Tourism Corporation Virginia Economic Development Partnership
Dams	Natural Resources	* Department of Conservation and Recreation Department of Game and Inland Fisheries
Emergency Services	Public Safety	* Department of Emergency Management Department of State Police
Commercial Nuclear Reactors, Materials, and Water	Natural Resources Public Safety	* Department of Emergency Management Department of Conservation and Recreation Department of Game and Inland Fisheries Department of State Police Department of Health
Information Technology	Technology	* Information Technologies Agency
Telecommunications	Technology	* Information Technologies Agency State Corporation Commission
Postal and Shipping	Transportation	* Department of Transportation
Transportation Systems	Transportation	* Department of Transportation
Critical Manufacturing	Commerce and Trade	*Department of Business Assistance Virginia Economic Development Partnership Department of Transportation

Government Facilities	Administration	* Department of General Services Department of State Police Department of Military Affairs

Figure 10: Commonwealth of Virginia Sector Specific Agencies

The State Sector Specific Plans provide details on how the CIKR mission will be coordinated, developed, and implemented within the 18 State CIKR sectors. These plans will continue to evolve as threats change and protective programs are implemented. Because each State sector has unique issues and concerns, preferred approaches to protection vary within and across State CIKR sectors. State Sector Specific Plans are tailored to address the unique characteristics and risk landscapes of each State sector while also improving consistency for protective programs, public and private protection investments, and resources. State Sector Specific Plans serve to:

- Define Federal and State sector security partners, authorities, regulatory bases, roles and responsibilities, and interdependencies;
- Establish or institutionalize existing procedures for federal and State sector interaction, information sharing, coordination, and partnership;
- Establish the goals and objectives, developed collaboratively with federal and state security partners, required to achieve the desired protective posture for the sector;
- Identify national and international considerations; and
- Identify the state sector-specific approach or methodology to be employed by the State Sector-Specific Agencies, in coordination with the Office of Commonwealth Preparedness (OCP).

The State Sector Specific Plans are sector-based documents in which the State Sector-Specific Agency coordinates with security partners and Sector Coordinating Committees, to develop a plan that highlights the State sector-specific approach to CIKR protection. In future years, the State Sector-Specific Agencies, in coordination with applicable security partners and Sector Coordinating Committees, will establish the mechanism to coordinate State Sector Specific Plan revision and update in accordance with the process established in the *VA Plan*. The OCP, as the overall State coordinator for CIKR protection, regularly monitors the *VA Plan* and State Sector Specific Plan implementation actions and tracks progress and success toward achieving the *VA Plan* goals and objectives.

Achieving the goals and objectives set forth in the *VA Plan* requires understanding and sharing information about terrorist threats and other hazards, building security partnerships, establishing Sector Coordinating Committees, implementing a long-term risk management program, and maximizing the efficient use of resources. The State Sector Specific Plans enable that by establishing, for each state sector, a means of managing risk by setting security goals, assessing

risks, prioritizing CIKR, implementing vulnerability reduction programs, and measuring effectiveness to provide continuous feedback. This feedback loop, in turn, allows continuous refinement of the state CIKR protection program to address emerging priorities and contingencies, both now, and in the future.

All State Sector Specific Plans will adhere to the following framework.

State Sector Profile and Goals

This section provides a characterization of the state sector, identifies security partners, Sector Coordinating Committees and their roles and responsibilities, and describes the sector's goals and desired long-term security posture. It is designed to help readers of the State Sector Specific Plan to understand the nature and complexity of the State sector, the current status of relationships among sector partners, the state sector's security goals, and the existing regulatory environment. The OCP uses this information to understand sector responsibilities, obtain information on the key security partners and Sector Coordinating Committee members, in the state sector and how they relate to each other, and understand the state sector goals for CIKR.

Identify Assets, Systems, Networks, and Functions

This section of the State Sector Specific Plan explains the processes that the State Sector-Specific Agency and the OCP will use to identify assets, systems, networks, and critical functionality, and to collect information pertinent to risk management. The focus is on those assets, systems, networks, and functions that if damaged would result in significant consequences – impacts on national economic security, national public health and safety, public confidence, loss of life, or some combination of these adverse outcomes. Throughout this section, the State Sector Specific Plan pays specific attention to the roles and responsibilities of the various sector security partners and owner/operators, as well as protection mechanisms.

Assess Risks

This section of the State Sector Specific Plan describes the processes and methodologies used by the sector to assess risk in support of three levels of protective activities:

Cross-sector protection efforts, typically coordinated by the OCP or local governments when multiple sectors of concern exist in their locations;

Sector or subsector-specific protection efforts, typically coordinated by the State Sector-Specific Agency, other state agencies, or industrial associations; and

Asset-, system-, or network-specific protection efforts, typically coordinated by the asset, system, or network owner or operator.

Prioritize Infrastructure

This section describes the state sector's process for risk-based prioritization of assets, systems, networks, and the functions they provide within the sector. This section focuses on the prioritization processes that support state sector-specific protection efforts.

Develop and Implement Protective Programs

This section describes how various state sector security partners and owner/operators will develop and implement protective programs throughout their state sector. It focuses on the process used to identify, assess, select, and implement protective programs, as opposed to presenting an extensive discussion of protective programs currently in place. It is not expected that the State Sector-Specific Agency will be solely responsible for development and implementation of protective programs. The State Sector-Specific Agency should facilitate the effective implementation of protective programs by coordinating with its private sector and other security partners.

Measure Progress

This section of the State Sector Specific Plan describes how the state sector intends to measure risk management progress and how this information will be used to support continuous improvement in state sector CIKR protection and risk mitigation efforts. Measuring progress is the shared responsibility of the OCP, the individual State Sector-Specific Agencies, and the State sector's security partners. While the OCP focuses on measuring progress across all CIKR State sectors, each State Sector-Specific Agency is responsible for measuring progress for its own state sector or subsectors. This section of the State Sector Specific Plans focuses on state sector-specific metrics and how the State Sector-Specific Agency and its security partners will meet the collection, verification, and reporting requirements of the core National Infrastructure Protection Plan and the *VA Plan* metrics.

Critical Infrastructure Key Resource Sector-Specific Plan

Executive Summary

Introduction

- Structured planning helps organize the thought process throughout the planning and execution of CIKR protection
- Planning should:
    - Focus on the sector mission and the threat
    - Support decision making throughout crisis management
    - Direct and coordinate actions
    - Develop a shared situational awareness
    - Generate expectations about how actions will evolve and how they will affect the desired outcome
    - Support the exercise of initiative
    - Shape the thinking of planners

1. Sector Profile and Goals
    a. Sector Profile

    Mission—State the sectors mission in regards to CIKR protection. (Should be specified in VA Plan)

        - Analyze orders, guidance, and other information provided by Federal and State governments to produce a sector mission statement
        - Identify sector's purpose and essential tasks
        - Identify additional information requirements
        - Identify constraints/restraints—actions that Sector must do/cannot do
        - State assumptions

    b. Security Goals

        - Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.
        - Examination of sector profile and mission statement guides goal development
        - Define protective postures (Refer to BZPP, COOP) in terms of objective metrics

- Separate goals may need to be considered for specific assets, systems, networks, etc.

2. Identify Assets, Systems, Networks, and Functions
    - Develop an inventory of the assets, systems, and networks, including those located outside the State, that comprise the State's CIKR and the critical functionality therein; collect information pertinent to risk management that takes into account the fundamental characteristics of each sector.
    - Consider inter/intra sector dependencies
    - Identify owners and stakeholders
3. Assess Risks

Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazard(s) (including seasonal changes in consequences, and dependencies and interdependencies associated with each identified asset, system, or network), known vulnerabilities to various potential attack vectors, and general or specific threat information.

- Assess Risk as a function of Consequence, Vulnerability and Threat
    - R=f(C,V,T)
    - Consequence Analysis
        - Human
        - Economic
        - Public Confidence
        - Government capability
    - Vulnerability
        - Determine appropriate strategy and methodology
        - Use common threat scenarios
        - Consider dependencies and interdependencies with other assets and sectors
    - Threat
        - Calculated based on the likelihood of occurrence of attack or natural damage on a particular asset, system, or network
        - HITRAC data supports all Sectors
        - Review DHS Sector Specific Threat Assessments
            - Terrorist Target Selection Matrix
            - Attack-Specific Threat Scenarios

        - Plan for continual updates to maintain awareness of incident reports and threat warnings
    - Focus assessments on assets, system, networks and functions identified in step 2
    - Refer to DHS guidance and tools for calculating comparable estimates of risk (RAMCAP)
    - Collaborative process with CIKR owners and operators

4. Prioritize Infrastructure

Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk; establish priorities based on risk; and determine protection and business continuity initiatives that provide the greatest mitigation of risk.

- Determines which sectors, regions, or other aggregation of CIKR assets, systems, networks, or functions are subject to the highest risk as calculated using the NIPP risk management framework
- Determines which protective actions are expected to provide the greatest mitigation of risk for any given investment
- DHS Annual Risk Analysis Methodology Report provides process
- Judgment is critical to complex assessments of aggregate levels

5. Develop and Implement Protective Programs

Select sector-appropriate protective actions or programs to reduce or mange the risk identified; secure the resources needed to address priorities

6. Measure Progress

Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national CIKR protection program in improving protection, managing risk, and increasing resiliency

7. CIKR protection R&D
8. Sector Management and Coordination Appendices